An Information Security Risk Management Model for Smart Industries

Nader SOHRABI SAFA[a,1] , Carsten MAPLE[b] , Tim WATSON[c]
[a,b,c] *Cyber Security Centre at WMG, University of Warwick, Coventry, United Kingdom*

Abstract. Internet of Things (IoT) has been acknowledged as a new revolution in technology. IoT play an important role in the flourishing of smart manufacturing and in supply chains. However, information security is a controversial issue in this domain. In this paper, a novel information security management model is presented that shows how an appropriate threat model and risk model can mitigate the risk of information security breaches in an industrial environment. Risk identification based on organisational assets, analysis, evaluation, and treatment along with scope specification considering risk management in ISO/IEC 27005, HTRA, CORAS and OCTAVE Allegro have been considered in the framework development. The presented model mitigates the risk of information security for both service providers and service consumers in this environment. At the end of the paper, we highlight the ways in which the current research supplies us with a direction for future research in this domain.

1. Introduction

Information security breaches are an important risk in supply chains that should be managed. Selling information about industrial designs, products, customers, experts and so forth, can have serious consequences such as loss of markets, reputation, competitive advantages, intellectual property and, in the worst-case scenario, bankruptcy[1]. It is acknowledged that human and managerial aspects of information security should be considered alongside technological aspects of information security in order to ensure a more secure environment for information [2]. Integrity and collaboration in supply chains improves productivity, where the flow of information plays an important role in this regard. However, this can create a risk for information leakage [3]. Information security management in supply chains identifies, prevents, and predicts information security risks and mitigates and decreases the negative consequences of information security breaches [4]. Identification of threats and the risks associated with them are extremely important in supply chains. That is why threat models and risk models are basic parts of our framework.

In the modern supply chain the Internet and smart devices play important roles, and cyber security covers more subject-matter than only information security [5]. Different smart objects exchange information; device identification, secure communication, and trust formation (data accuracy and proper functionality of devices) are examples of important subjects in supply chain cyber security.

Corresponding author is Nader Sohrabi Safa, n.sohrabi-safa@warwick.ac.uk

2. Research Methodology

Threat modelling and risk modelling are two important parts of the information security management model in this study. The threat model aims to improve awareness and identification of all plausible threat scenarios that may affect a particular online service in the environment [6]. Asset identification, vulnerability, threats and environment characteristics were considered for threat identification and modelling. Assets and security controls were taken into account in every environment. Relevant risks are identified which are related to possible threats. Every risk description is based on a threat, environment, asset, vulnerability, and risk score and recovery activities. Each activity is characterised by priority, status, and its outcomes.

The scope of the model covers the threats that influence service providers and service consumers. Threat agents that exist in third party environments can influence assets in the other parties. The model covers threats and assets based on cause and effect relationships that may result in particular incidents. Asset's and agent's characteristics play important roles in the threat modelling. Vulnerability of an asset originates from threat ability and characteristics. Figure 1 shows relationship between threats, assets and risks.

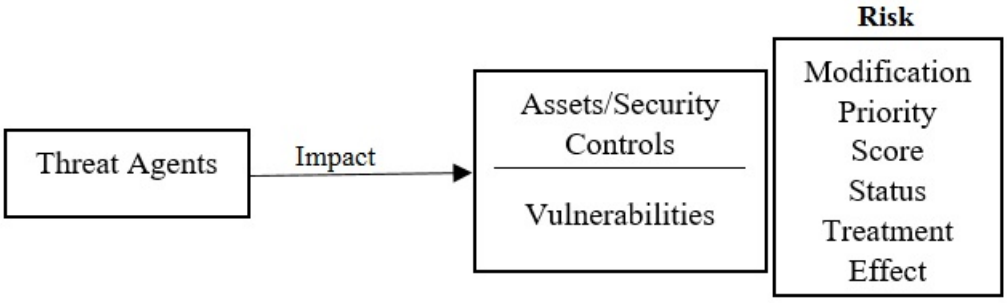

Figure 1: Threats, assets, and risks in the model

Any valuable and useful entity that contributes directly or indirectly to business functionality is an asset. From this point of view, a security control that protects a specific asset is considered as an asset by the model. Descriptions of the assets in the proposed model are presented in the Table 1.

Table 1: Assets description

Assets	Descriptions
Individuals	People who operate, provide and consume online services.
Governance	This covers business and ICT levels.
Process	All activities and process that are related to service providers and service consumers.
Technology	Software and hardware utilised for online service providers and consumers.
Information	Information assets that are presented by data or stored by technology in the system.

The assets in a smart supply chain may be located in:

1) The service provider's environment
2) The service consumer's environment
3) The partner's environment

3. Threat Model

A threat agent is an entity that has the ability or potential to negatively influence online service security with respect to any element of the supply chain. Insiders and outsider threats are hot topics in this domain and have recently attracted the attention of experts [7]. Insider threat refer to any illegal transfer of information to unauthorised parties for any reason. Selling information for monetary benefit, getting revenge, satisfaction (by disgruntled employees), bayberry, embezzlement, and espionage are examples of motivations for information leakage in supply chains [8]. The lack of awareness, negligence, apathy, mischievousness, resistance, and even entertainment have been mentioned as reasons for information security breaches by employees. Technology also harbours a great potential for threats to information: virus, denial of service attack, spoofing, sniffer attack etc. are examples of such technological threats. Table 2 shows the definition of the various threats in a concise form.

Table 2: Threat agents description

Threat Agents	Description
Human	Human intentionally or unintentionally are a great potential of risk in every environment for information.
Technology	The threats such as malware activities, malfunctions or failures that jeopardise processes, information, and other activities.

We define a vulnerability as a weakness of control of an asset that originates from a threat agent in the supply chain.

4. Risk Model

The aim of the risk model is to identify, assess and treat risks regarding information security in the supply chain. Threats based on scenario is a useful approach that helps experts to identify and mitigate risks. Threat agents and their effects are identified as part of a scenario. Different types of threats are mapped to asset types and based on the output of this section knowledge and awareness will be improved. In a proper scenario based risk modelling the hidden aspects of a threat will be disclosed.

The quantitative risk analysis method is another useful approach that has been mentioned in ISO/IEC 270075:2011. A three-level scale is used for describing the likelihood and impact levels which create five levels of possible risk severity and nine risk scores. Figure 2 shows risk management model.

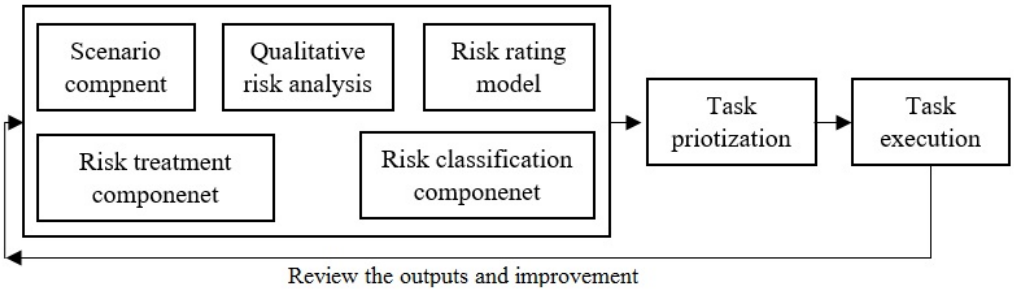

Figure 2: Risk management model

Identification of vulnerability is an important task in the risk management process, but estimation of risk severity to the business contributes to better decision making. Having a system for the rating of risks saves time and creates better view to prioritize the tasks for treatment. This system helps us to be sure that the business process will not be inhibited by risk, ignoring more serious risks. OWASP is a common approach to risk analysis that contains risk identification, estimating likelihood based on factors, estimating impact, determining the severity of risk, treatment and improvement of risk rating system. Based on this the risk severity, score and likelihood is presented in Table 3.

Table 3: Impact, likelihood, risk severity and scores

	Low impact (value 3)	**Medium impact (value 6)**	**High impact (value 9)**
High likelihood (value 6)	Medium risk (score 9)	High risk (score 12)	Critical risk (score 15)
Medium likelihood (value 4)	Low risk (score 7)	Medium risk (score 12)	High risk (score 13)
Low Likelihood (value 2)	Very low risk (score 5)	Low risk (score 12)	Medium risk (score 11)

The Delphi method used in order to test the reliability of the presented model. The approach and the model were sent to several experts in the domain of information systems, information security and supply chain management. We improved the model based on their feedback.

5. Non-Technological Aspects of Information Security

Technology has positively affected information security. That is why attackers have shifted their attention and efforts towards the human elements to achieve their targets. In this dynamic environment, users' information security awareness and knowledge play important role in mitigating the risk of information security [9]. Experts divided information delivery methods into three groups – contextual, web-based material and embedded training methods. Video-based, game-based, and text-based delivery methods are other types of methods that increase the information security knowledge and awareness of users [10].

The prevention of damage, loss, unauthorised access or destruction of information is vital for organisations. External and internal threats continually grow and result in breaches. Employees behaviour is the root of many information security breaches [11]. Reliable reports show that internal threats have significantly increased in comparison with previous years [12, 13]. Users error, negligence, and intentionally malicious attacks are reasons for information security breaches. [14] categorises users behaviour in four categories – security assurance behaviour, security damage behaviour, security risk-taking behaviour, and security complaint behaviour. The management of human error should be a priority in organisations. A strong information security culture can contribute to mitigating vulnerability caused by the behaviour of individuals [15]. Infrequent back-up of information, using email accounts to send sensitive and confidential information, carrying sensitive and confidential information on external hard disk or other movable devices unencrypted, unlawful use of information, and the unauthorised transference of information are problems that that can be solved by enforcing a proper information security culture [16]. Information security culture covers the entire information life cycle – collection, storage, use, and transfer. Regulatory requirements, customer preferences and expectations, and geographical distribution are external factors that influence information security culture [11]. Regulation protecting personal and financial information influences customer information processes. This determines how long customer records should be kept. Values, attitudes, norms, assumptions, beliefs and knowledge are important factors in culture formation. Protection of information and privacy is valuable in information security culture. The illegal transfer of information to unauthorised parties is a negative behaviour (attitude). Everybody knows that he or she should put his/her effort into avoiding any behaviour that jeopardises information confidentiality (assumption).

6. Conclusion

New technologies help experts to connect people and things to each other anytime and anyplace using any network and service. In another words, world and virtual entities communicate in order to achieve a target. They can share information resources, services and create a new group or network. Objects can negotiate and adopt to their environment and extract patterns and information. They can learn and make decisions. They have the abilities to self-replicate, control, create, manage and even destroy. However, aside from the many advantages for us that this new revolution brings, there are some challenges that should be addressed by experts, such as:

- IoT devices do not have malware detection or prevention capability.
- IoT has the potential to increase network traffic.
- Any object can connect to the IoT network, and hence it is a jumping off point for an attack.
- Non-uniform devices can connect to the IoT network.
- Data that is generated by a sensor is an asset that should be protected.
- The danger of ransomware that controls and blocks access to an object is expertly important in IoT.

There are a variety of identified and un-identified risks in this environment. It is necessary for different potential risks to be predicted, identified, responded to on-time and the lessons

of these events be used for the future by Information Security Response Teams (ISRTs). An intelligent information security system that makes the right decisions, based on accurate data, can help to mitigate the risk of information security breaches. This provides us with a direction for future research. A further topic of investigation for future research suggested by the current work is an investigation of how to use the risk detection approach and algorithm, multicriteria decision making, and risk prioritisation methods, in order to flag-up potential security breaches for different parts of production system.

References

1. Lee, J., U.S. Palekar, and W. Qualls, *Supply chain efficiency and security: Coordination for collaborative investment in technology.* European Journal of Operational Research, 2011. **210**(3): p. 568-578.
2. Safa, N.S., et al., *Information security conscious care behaviour formation in organizations.* Computers & Security, 2015. **53**(0): p. 65-78.
3. Tan, K.H., W.P. Wong, and L. Chung, *Information and Knowledge Leakage in Supply Chain.* Information Systems Frontiers, 2016. **18**(3): p. 621-638.
4. N, S.P. and A.S. Kunnathur, *Information security in supply chains: a management control perspective.* Information and Computer Security, 2015. **23**(5): p. 476-496.
5. Von Solms, R. and J. Van Niekerk, *From information security to cyber security.* Computers & Security, 2013. **38**(0): p. 97-102.
6. Meszaros, J. and A. Buchalcevova, *Introducing OSSF: A framework for online service cybersecurity risk management.* Computers & Security, 2017. **65**: p. 300-313.
7. Blasco, J., et al., *Bypassing information leakage protection with trusted applications.* Computers & Security, 2012. **31**(4): p. 557-568.
8. Safa, N.S. and C. Maple, *Human errors in the information security realm – and how to fix them.* Computer Fraud & Security, 2016. **2016**(9): p. 17-20.
9. Haeussinger, F.J. and J.J. Kranz. *Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior*. in *International Conference on Information Systems 2013*. 2013.
10. Abawajy, J., *User preference of cyber security awareness delivery methods.* Behaviour & Information Technology, 2014. **33**(3): p. 236-247.
11. Da Veiga, A. and N. Martins, *Information security culture and information protection culture: A validated assessment instrument.* Computer Law & Security Review, 2015. **31**(2): p. 243-256.
12. Schulze, H., *Insider Threat Spotlight Report*. 2015, Information Security Community on LinkedIn. p. 1-36.
13. Verizon, *Data Breach Investigations Report (DBIR 2016)*. 2016, Verizon: United States. p. 1-70.
14. Guo, K.H., *Security-related behavior in using information systems in the workplace: A review and synthesis.* Computers & Security, 2013. **32**: p. 242-251.
15. AlHogail, A., *Design and validation of information security culture framework.* Computers in Human Behavior, 2015. **49**: p. 567-575.
16. Van Niekerk, J.F. and R. Von Solms, *Information security culture: A management perspective.* Computers & Security, 2010. **29**(4): p. 476-486.